IPv6 네트워크와 IPv4 네트워크 연동을 위한 NAT-PT 에서의 IPsec 지원 기법

김정열*, 김대선**, 홍충선***
경희대학교 컴퓨터공학과
e-mail : jykim102@networking.khu.ac.kr*, dskim@.khu.ac.kr**,
cshong@khu.ac.kr***

IPsec Support Mechanism between IPv6 Network and IPv4 Network Communication using NAT-PT

Jung Youl Kim*, Dae Sun Kim**, Choong Seon Hong***
Dept. of Computer Engineering, Kyung Hee University

요 약

IPv6 의 도입으로 인해 상당기간 IPv4 와 공존해야 한다. 따라서 IPv4 와 IPv6 간 변환 기술이 필요로 하게 되었으며 이에 여러 가지 변환 기술이 제안되어 두 프로토콜간 통신이 가능하게 되었다. 그 중 NAT-PT 는 IPv6 기반의 네트워크와 IPv4 기반의 네트워크간에 직접 통신이 가능하도록 해주는 메커니즘이다. 그러나 IPsec 프로토콜의 인증 값 계산에는 TCP/UDP/ICMP 검사합 값을 포함해서 IP 주소가 사용되기 때문에 NAT-PT 에는 IPsec 프로토콜을 적용할 수 없다는 보안상의 문제가 발생하였다. 따라서 본 논문에서는 NAT-PT 와 IPsec 의 특성을 살펴보고, NAT-PT 의 보안상 문제점을 고찰하였으며 NAT-PT 에 IPsec 을 적용할 수 있는 방안을 제안하였다.

1. 서론

IPv6[1]에 관한 연구가 각 분야에서 활발히 연구되고 있으며, 그 중 IPv4 와의 변환 기술에 관한 연구도 활발히 진행되고 있다. IPv6 를 도입하기 위해서는 기존의 IPv4 사용자들이 쉽게 IPv6 로 이동할 수 있게 도와주는 몇 가지 변환 메커니즘들이 필요로 하며, 그 중 NAT-PT(Network Address Translation - Protocol Translation)[3]는 IPv6 기반의 네트워크와 IPv4 기반의 네트워크 경계에서 IP 패킷의 헤더를 변환하여 그 둘 간의 통신을 지원하는 변환 메커니즘이다. NAT-PT 에서 헤더변환은 SIIT(Stateless IP ICMP Translation)[4]에 기술된 IPv4/IPv6 헤더 변환 규칙을 사용하고, 각 연결마다 임시로 할당할 IP 주소는 경계 라우터인 NAT-PT 의 address pool[3]에서 할당한다. 그러나 IPsec 프로토콜의 인증 값 계산에는 TCP/UDP/ICMP 검사합(Checksum) 값을 포함해서 IP 주소가 사용되기 때문에 NAT-PT 에 IP 계층의 보안 프로토콜인 IPsec[5]을 적용 할 수 없다는 문제가 발생하였다. 본 논문에서는 NAT-PT 의 보안상의 문제점을 고찰해 보고 해결 방안을 제시하였다.

본 논문의 구성은 다음과 같다. 2 장에서는 NAT-PT 의 기본 동작과정과 IPsec 의 AH(Authentication Header)[6], ESP(Encapsulating Security Payload)[7] 프로토콜의 특징을 소개한다. 3 장에서는 NAT-PT 에 IPsec 프로토콜을 적용하였을 경우 문제점에 대하여 기술하고, 본 논문에서 제안하는 NAT-Traversal[8][9] 방법을 NAT-PT 에 적용하는 방안은 4 장에서 설명한다. 마지막 5 장에서는 결론 및 향후 연구 계획으로 마무리 한다. 본 논문에서 기술된 내용은 TCP 뿐만 아니라 UDP 와 ICMP 에서도 모두 동일하다.

This work was supported by MIC and ITRC project.

2. 관련 연구

NAT-PT 는 IP 주소 변환과 TCP 헤더의 검사합 값을 갱신하며, IPsec 은 AH 와 ESP 를 사용하여 IP 계층에서 강력한 보안 서비스를 제공한다.

2.1 NAT-PT.

IPv6 기반의 노드가 IPv4 기반의 노드로 패킷을 전송할 경우, DNS-ALG[3]의 도움으로 IPv4 DNS 서버로부터 목적지 IPv4 주소를 획득하고, 송신용 IPv4 주소를 NAT-PT address pool 로부터 할당 받은 후, NAT-PT 에서 할당 받은 PREFIX 로 IPv6 주소[3]를 구성하여 패킷을 전송한다. NAT-PT 에 도착한 패킷은 address pool 에서 할당한 IPv4 주소와 PREFIX 를 제거한 IPv4 주소로 변환되고, TCP 헤더의 검사합을 갱신하여 패킷을 IPv4 노드에게 전송한다.

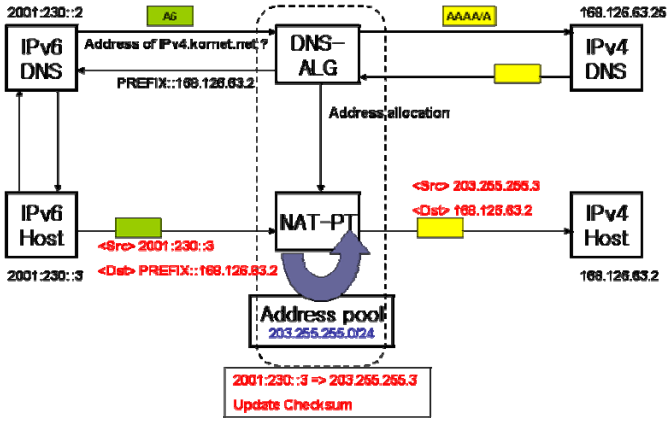

그림 1. NAT-PT 의 동작 과정

TCP 헤더의 검사합 값을 계산할 때에는 의사 헤더(PseudoHeader), TCP 헤더, 응용계층으로부터 온 데이터의 세 부분을 포함한다. 의사 헤더에는 IP 의 발신지 주소와 목적지 주소가 포함되어 있으므로 NAT-PT 는 TCP 헤더의 검사합을 반드시 갱신해야만 한다.

2.2 IPSec AH.

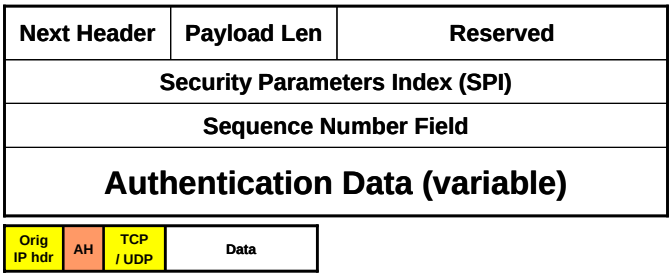

그림 2. AH 프로토콜 헤더의 구조

IPsec 에서 보안 서비스 제공을 위한 프로토콜은 AH 와 ESP 가 있다. AH 는 접근 제어(Access Control), 비 연결형 무결성(Connectionless Integrity), IP 데이터 그램에 대한 데이터 발신 인증(Data Origin Authentication) 등의 보안 서비스를 제공하며, 선택적으로 재전송 공격 방지(Anti-Replay) 서비스를 제공할 수 있다. 그림 2 는 AH 프로토콜 헤더의 구조와 ICV(Integrity Check Value)[6] 계산에 포함되는 부분을 나타내었다. AH 는 IP 헤더 필드와 AH 헤더, 그리고 상위 계층의 프로토콜 헤더의 정보를 사용하여 ICV 를 계산한 다음 Authentication Data 필드에 삽입한다. ICV 계산에는 HMAC(Keyed-Hashing for Message Authentication)[12]과 MD5(Message Digest)[13], 또는 SHA-1(Security Hash Algorithm) 알고리즘이 결합된 HMAC-MD5 와 HMAC-SHA-1 알고리즘을 사용한다.

2.3 IPSec ESP

ESP 헤더는 페이로드에 대해서 AH 가 제공하는 서비스 외에 추가적으로 비밀성(Confidentiality) 서비스를 제공한다.

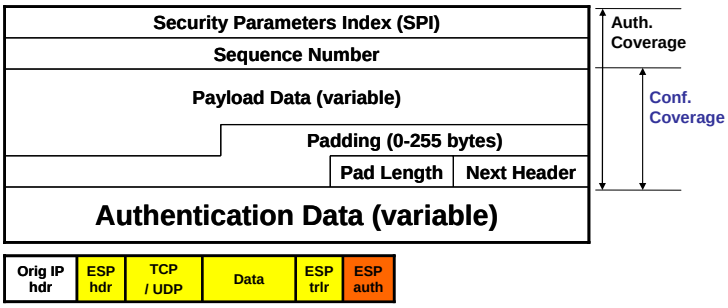

그림 3. ESP 헤더의 구조

그림 3 은 ESP 프로토콜 헤더의 구조와 ICV 계산에 포함되는 부분을 나타내었다. ESP 는 페이로드 필드부터 Next Header 필드까지 암호화하며, AH 와는 달리 ICV 계산에 IP 헤더 필드를 사용하지 않고, ESP 헤더에 포함되는 필드만을 사용한다. ESP 의 암호화 알고리즘에는 CBC(Cipher Block Chaining) 모드의 3DES(triple Data Encryption Standard)[14] 알고리즘을 사용한다.

2.4 HTI(Header Translation Information) 메시지 사용 기법

NAT-PT 에 IPsec 을 적용하기 위해서 IKE 협상과정 중 HTI[11] 메시지를 사용하는 기법이 제안된 바 있다. 이 알고리즘에서는 NAT-OA(NAT Original Address)[8] 페이로드를 사용하지 않고 IKE(Internet Key Exchange)[10] 협상 패킷이 NAT-PT 로 전달되면, NAT-PT 가 새롭게 정의된 HTI 메시지를 사용하여 Initiator 에게만 Responder 의 실제주소를 전달한

다. 그 후 패킷의 송신 노드가 NAT-PT 로부터 받은 수신 노드의 실제주소를 사용하여 NAT-PT 에 의해 갱신되는 TCP 헤더의 검사합 값을 예측 계산함으로써 NAT-PT 에 IPsec 적용 방법을 제안 하였다. 그러나 이 알고리즘은 UDP 헤더로 ESP 패킷을 캡슐화하는 과정이 없으므로, NAT-PT 에 의해 TCP 헤더의 검사합 값이 갱신되고, 수신측이 그 갱신된 TCP 헤더의 검사합으로 ICV 를 계산하면 ICV 에 차이가 생기게 된다. 따라서 패킷은 TCP 헤더의 검사합 값을 재수정하기 전에 버려진다. 또한, 패킷의 송신측이 TCP 헤더의 검사합 값을 미리 예측하여 계산하는 방법은 본 논문이 제안하는 NAT-PT Traversal 에서도 가능하며, 수신측에서 최종적으로 TCP 헤더의 검사합 값을 재 수정하는 과정이 수신측에서 진행되지 않고 송신측에서 처리될 뿐 큰 의미는 없다.

3. NAT-PT 에 IPSec 적용시 문제점

NAT-PT 에 IPsec 적용시 문제점은 AH 를 사용할 경우와 ESP 를 사용할 경우, 두 가지로 나누어 생각해 볼 수 있다.

3.1 Authentication Header

그림 2 에서 보는 것과 같이 AH 는 ICV 계산에 IP 헤더의 값과 TCP 필드의 값을 사용한다. 따라서 NAT-PT 에 의해 IP 헤더의 출발지 주소와 목적지 주소가 변환되면 수신측은 ICV 검증과정에 변환된 IP 헤더의 출발지 주소와 목적지 주소를 사용하므로 계산된 ICV 가 틀려지게 되고 패킷은 버려진다. 뿐만 아니라 NAT-PT 에 의해 추가적으로 갱신된 TCP 헤더의 검사합 값도 수신측의 ICV 계산에 사용되므로 검증과정에서 계산된 ICV 는 수신된 패킷의 ICV 와 차이가 있다.

3.2 Encapsulating Security Payload

ESP 헤더는 그림 3 에서 보는 것과 같이 ICV 계산에 ESP 헤더에 포함되는 부분만을 사용하므로 AH 처럼 IP 주소 변환에 의한 문제는 없다. 그러나 TCP 헤더의 검사합 값이 ESP 헤더에 포함되므로, AH 와 마찬가지로 NAT-PT 에 의해 갱신된 TCP 헤더의 검사합 값을 수신측의 ICV 검증과정에서 사용하게 되면 문제가 발생한다.

4. NAT-PT Traversal 제안

NAT-PT 는 NAT(Network Address Translation)[2]를 기반으로 하는 기술이기 때문에 그 성질 또한 NAT 와 크게 다르지 않다. 이에 본 논문에서는 NAT 에서 사용되고 있는 NAT 를 통과하기 위한 IKE 협상과 IPsec ESP 패킷을 UDP 헤더에 캡슐화 하는 기법을 통하여 NAT-PT 에 IPsec ESP 프로토콜을 적용하는 NAT-PT Traversal 방안을 제안 하였다.

4.1 NAT-PT 를 통과하기 위한 IKE 협상

IKE 협상과정 중 NAT 에서 사용되고 있는 Quick Mode 의 NAT-OA(NAT Original Address)[8] 페이로드를 이용하여 IPv6 기반의 노드와 IPv4 기반의 노드들은 IPsec 에 사용된 실제의 주소를 서로 주고받을 수 있다. 따라서 각 노드들은 NAT-OA 를 통해 획득한 실제 주소를 사용하여 TCP 헤더의 검사합 값을 재 수정할 수 있다.

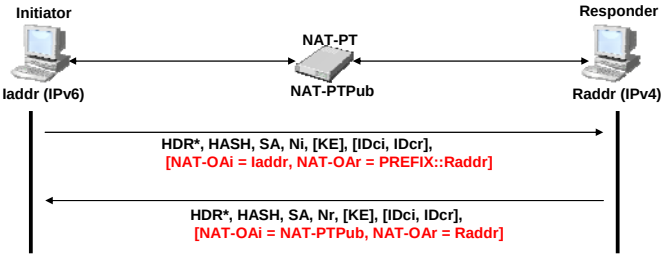

그림 4. IKE 의 NAT-OA 를 통한 NAT-PT Traversal 동작 과정

그림 4.는 NAT-OA 페이로드를 사용하여 실제 주소를 주고받는 과정이다. laddr 는 IPv6 노드의 실제 주소이고, Raddr 은 IPv4 노드의 실제 주소, 그리고 NAT-PTPub 는 NAT-PT 에 의해 할당 받은 IPv6 노드의 IPv4 주소이다.

① Initiator (IPv6 nodes)
- NAT-OA initiator = laddr = IPv6 node's original address
- NAT-OA responder = Raddr = PREFIX::IPv4 node's original address

② Responder (IPv4 nodes)
- NAT-OA initiator = NAT-PTPub = IPv6 node's assigned address by NAT-PT address pool
- NAT-OA responder = Raddr = IPv4 node's original address

4.2 IPsec ESP 패킷을 UDP 헤더로 캡슐화

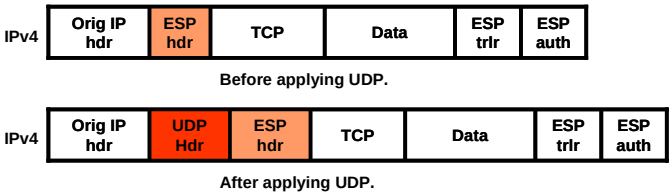

그림 5. UDP 헤더로 캡슐화된 ESP 패킷

NAT-PT 가 ESP 헤더안쪽의 TCP 검사합 값을 갱신하지 못하도록 그림 5 와 같이 UDP 헤더로 ESP 패킷을 캡슐화한다.

► UDP 헤더 캡슐화 하는 절차
① ESP 캡슐화
② UDP 헤더를 ESP 헤더 앞에 삽입
• UDP 헤더의 검사합 값을 0 으로 설정하면 UDP 헤더의 검사합 갱신 없이 NAT-PT 를 통과 할 수 있다. (IPv4 노드만 해당)
③ IP 헤더의 Total Length, Protocol, 그리고 Header Checksum 필드를 삽입된 UDP 헤더에 맞추어 수정 (IPv4 노드만 해당)

► UDP 헤더 역 캡슐화 하는 절차
① UDP 헤더 제거
② IP 헤더의 Total Length, Protocol, 그리고 Header Checksum 필드를 기존의 IP 헤더 값으로 수정 (IPv4 노드만 해당)
③ ESP 역 캡슐화 과정

따라서 ESP 헤더 안의 모든 필드는 어떠한 변경도 없이 NAT-PT 를 통과할 수 있다.

4.2 TCP 헤더의 검사합 값 재수정

검사합 값의 갱신 없이 NAT-PT 를 통과한 TCP 헤더의 검사합은 ESP 의 ICV 검증에는 문제가 없으나, 수신측에서 TCP 헤더의 검사합을 검증하는데 의사헤더를 참조하므로 여전히 문제가 남아있다. 이러한 문제를 해결하기 위해서 IKE 협상 과정에서 주고받은 실제 주소를 사용하여 TCP 헤더의 검사합 값을 재수정한다. 수정하는 과정은 다음과 같다.

① 수신된 패킷의 TCP 헤더의 검사합 값으로부터 IP 헤더의 출발지 주소를 뺀다.
② TCP 헤더의 검사합 값에 NAT-OA 를 통해서 획득한 실제 출발지 주소를 더한다.
③ 수신된 패킷의 TCP 헤더의 검사합 값으로부터 IP 헤더의 목적지 주소를 뺀다.
④ TCP 헤더의 검사합 값에 NAT-OA 를 통해서 획득한 실제 목적지 주소를 더한다.

5. 결론 및 향후 과제

본 논문에서는 IPv6 기반의 네트워크와 IPv4 기반의 네트워크가 NAT-PT 를 사용하여 통신할 시에 IPsec 의 인증 값 계산으로 TCP/UDP/ICMP 검사합 (Checksum) 값을 포함해서 IP 주소가 사용되기 때문에 일어나는 NAT-PT 와 IPsec 의 비호환성 문제를 분석하였고, 이를 해결하는 방안으로 NAT 에서 사용되고 있는 NAT 를 통과하기 위한 IKE 협상과 IPsec ESP 패킷을 UDP 헤더에 캡슐화 하는 기법을 통하여 NAT-PT 의 보안상의 문제점을 해결할 수 있는 방안을 제안하였다.

향후 과제로는 NAT-PT 의 주소변환 과정이 아닌 헤더변환 과정(SIIT)에 의한 여러 가지 상황에서 NAT 를 통과하기 위한 IKE 협상과 IPsec ESP 패킷을 UDP 헤더에 캡슐화 하는 기법의 사용이 NAT 에서와 같이 NAT-PT 에서도 가능한 것인지 구현을 통한 검증이 필요하다.

참고문헌

[1] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
[2] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, May 1994.
[3] G.Tsirtsis, et al., "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000
[4] E. Nordmark., "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, February 2000.
[5] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 1825, November 1998.
[6] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.
[7] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
[8] T. kivinen, B. Swander, A. Huttunen, V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.
[9] A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.
[10] D. Harkins, D. Carrel, “The Internet Key Exchange (IKE)” RFC 2409, November 1998
[11] 최인석, “IPv6 전환 기술의 보안 분석 및 보안 설계에 관한 연구”, December 2004.
[12] H. Krawczyk, M. Bellare, and r. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.
[13] R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992
[14] C. Madson, and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm with Explit IV", RFC 2405, November 1998.